图书情报工作
第63卷 第3期 2019年2月
ChinaXiv合作期刊

云计算环境下学术信息资源共享全面安全保障机制*

■ 石宇 胡昌平
武汉大学信息管理学院 武汉 430072

摘要：[**目的/意义**]从技术和管理角度构建云计算环境下学术信息资源共享全面安全保障机制,从而指导共享安全保障实施。[**方法/过程**]通过分析云计算环境下学术信息资源共享流程及安全要素,进行学术信息资源共享全面安全保障机制设计。[**结果/结论**]构建了基于学术信息资源共享流程安全技术保障机制及基于多主体协同的学术信息资源共享安全保障组织机制。

关键词：云计算环境 学术信息资源共享 安全保障机制
分类号：G251
DOI：10.13266/j.issn.0252-3116.2019.03.007

chinaXiv:202307.00609v1

云计算环境下,学术信息资源共享方式发生了重大变化,学术信息资源共享服务中各环节的安全问题日趋复杂,传统的安全保障策略无法保障云环境下学术信息资源共享的顺利进行。针对这一情况,本文结合云计算环境特征与学术信息资源特征,在分析云计算环境下学术信息资源共享流程及其安全要素的基础上,从技术及管理方面构建学术信息资源共享安全保障机制。技术保障机制方面,需要基于共享服务实施流程,从共享资源发布安全、组织安全、利用安全与撤销安全方面构建全流程技术保障机制,确保资源在共享的各个环节中的可用性、保密性、完整性;安全保障组织方面,利用多主体协同思想构建学术信息资源共享安全的保障组织机制,确定各安全保障主体及其定位,并通过各方高效协同,保障学术信息资源共享安全。

1 云计算环境下学术信息资源共享流程及安全要素

深入分析云计算环境下学术信息资源共享流程及其安全要素是构建学术信息资源共享安全保障机制的基础,本节将对云计算环境下学术信息资源共享实现流程进行梳理,在此基础上对学术信息资源共享过程中的安全要素及其交互关系进行分析。

1.1 云计算环境下学术信息资源共享实现流程

信息资源共享的实现流程即信息资源从其所有者通过一定介质到其利用者的过程[1]。云计算环境下,学术信息资源共享集中于云平台中进行,学术信息资源所有者将共享资源从本地上传到云平台之中,云平台对资源进行组织后,共享资源利用者在云平台中实现共享资源的利用,具体流程见图1。

从总体上看,云计算环境下学术信息资源共享流程是从共享资源所有者开始,到共享资源被利用者利用的整个过程,包括发起学术信息资源共享、云中共享资源组织、共享资源利用、共享资源修改、共享资源撤销或删除。首先,共享资源所有者发起学术信息资源共享,其中共享的资源既包括学术资源如学术文献、科研数据等,同时也包括科学研究过程中涉及的各类软件工具、用户共享的知识信息、用户的部分个人信息,共享方式可以是用户上传并同时设置为共享的资源,也可以是云平台中已经存在的用户私有资源设置为共享资源,在进行共享时,需同时对共享的范围及权限进行明确规定;其次,云平台对共享资源进行管理组织,包括对云中存储的共享资源进行关联组织、对共享的学术信息资源进行存储及共享资源存储中的重复数据删除等;再次,在共享资源利用阶段,云计算环境下的学术信息资源利用更多是在云平台中进行,其利用方式更加快速、高效,用户可以通过云平台提供的搜索、

* 本文系国家社会科学基金重大项目"云环境下国家数字学术资源信息安全保障体系研究"(项目编号:14ZDB168)研究成果之一。
作者简介:石宇(ORCID:0000-0001-6741-5487),硕士研究生,E-mail:1084174531@qq.com;胡昌平(ORCID:0000-0002-9491-2160),教授,博士生导师。
收稿日期:2018-06-27 修回日期:2018-08-24 本文起止页码:54-59 本文责任编辑:刘远颖

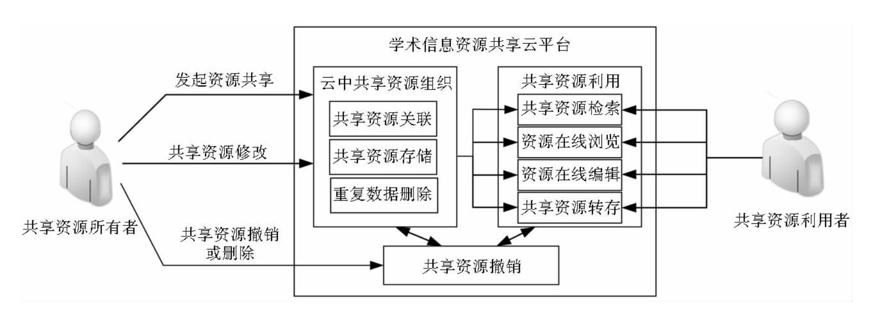


图1　云计算环境下学术信息资源共享流程

浏览服务获取所需的共享资源，并通过转存、在线浏览和编辑等方式进行利用；最后，共享资源的修改、撤销或删除阶段，其中共享资源的修改一般由共享资源所有者或拥有权限的用户在云平台中进行，在对共享资源修改后，需要重新限定资源共享的范围及权限，同时，共享资源所有者可以根据自身需求对资源进行撤销共享或删除，当共享资源撤销成用户私有资源或被共享资源所有者删除时，资源分享链接同时失效，云平台也可根据共享资源所有者的要求对其他副本资源进行传播范围控制、关联删除等限制，以保护共享资源所有者的知识产权。

1.2　云计算环境下学术信息资源共享安全要素及其交互作用

脆弱性、安全威胁和保障措施是直接影响信息安全的三类要素[2]。云计算环境下，学术信息资源共享充分利用云计算强大计算能力和快速伸缩的优势，在资源共享过程中表现出共享资源集中性、共享过程灵活性、共享服务可靠性的特点，即可提供统一在云平台上的、稳定高效的共享资源发布、获取及删改服务。但在其安全实现过程中，仍面临这三类要素的影响。同时，安全保障对象及安全保障主体这两方面直接影响这三类要素的形成，因此，在进行共享安全要素及其间的交互作用分析时，着重分析安全保障对象及安全保障主体对其的影响。

脆弱性一般指的是可能被攻击者攻击并产生安全事故的环节，一般由安全保障对象及其安全需求决定。根据《信息安全风险评估规范》，学术信息资源共享安全保障中的脆弱性可分为技术脆弱性和管理脆弱性两部分，技术脆弱性主要表现在资源传输、内容安全、访问控制与加密等方面，管理脆弱性包括组织安全、人员安全、共享资源所有者与云服务商的协同管理不健全等。云计算环境下，学术信息资源共享同时面临着传统计算环境及云计算应用环境下的安全威胁，主要包括基础设施故障、物理故障、操作不当、滥用权限、泄密、恶意篡改、网络攻击等，其中新的威胁包括隔离失效、数据主权威胁、经济型服务持续性拒绝攻击、责任不清、云服务商管理不到位、数据残留等威胁[3－5]。安全保障措施主要由安全保障主体提供，通常为有效的技术或管理方案。学术信息资源共享安全保障措施分为共享安全保障技术措施及共享安全保障管理措施，其中，技术包括密码技术、访问控制技术、虚拟化技术、内容安全检测技术等[6－8]。共享安全保障的管理实施既包括与安全技术相配合的安全管理组织，也包括关于人员、操作、设备等的规范化管理。

云计算环境下，学术信息资源共享安全要素与安全保障主体、安全保障对象间相互关联，共同对学术信息资源共享安全产生影响，对应的关系如图2所示：

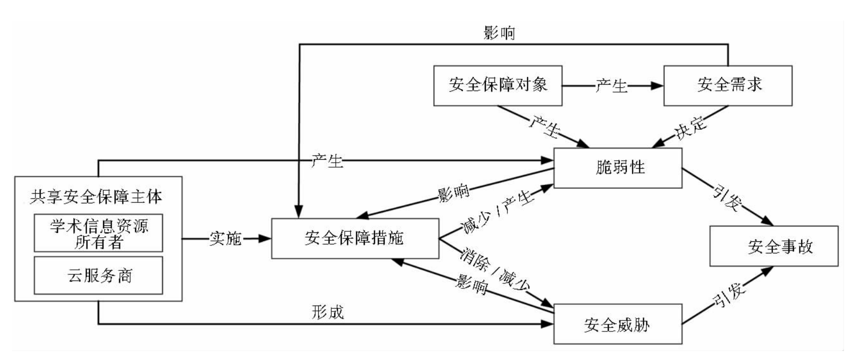


图2　云计算环境下学术信息资源共享安全要素间的交互

由图2可知，学术信息资源共享安全保障主体可能是脆弱性和安全威胁的来源，如当安全意识不足、操作失误、管理不完善时，会产生脆弱性及安全威胁，同时，安全保障措施一般是共享安全保障主体组织实施，由共享资源所有者与云服务商分工合作，针对学术信息资源共享过程中的脆弱性及安全威胁制定安全保障措施。安全保障对象是脆弱性的主要来源，其特征及安全需求决定了脆弱性。当安全威胁绕过或突破安全措施的保护，对学术信息资源共享过程中的某一环节的脆弱性发起攻击时，会引发安全事故，为避免其发生，一般可通过在脆弱性环节施加安全保障措施，以应对针对性的安全攻击。

从前面的分析可以得出学术信息资源共享安全保障需要从脆弱性和安全威胁出发，针对学术信息资源

chinaXiv:202307.00060v1

ChinaXiv合作期刊

共享流程，分析各个环节的脆弱性和安全威胁，施加安全保障措施。相应的安全保障措施需要充分考虑安全攻击发起的时间及产生的影响，进行较为全面的布置，即布置安全保障措施以预防安全攻击的产生，采取相应措施及时识别安全攻击以防止事故发生并造成危害，设定针对性方案以保障事故发生后共享资源及服务得以迅速恢复。同时，在对各阶段布置安全保障措施时，需采取技术与管理相结合的安全保障组织机制。在技术方面，布置的安全保障措施应将重点放在防御上面，针对共享过程中已经暴露出的脆弱性和安全威胁，可以选取有针对性的、有效的防御技术手段，避免类似安全事故再次发生，而对于还未发现的威胁和脆弱性，则采用监控的手段，并做好灾备管理，防止安全事故扩大。在管理方面，由于在云环境下，学术信息资源共享安全保障主体呈现多元化，因此需注重多主体间的协同管理，保障学术信息资源共享的顺利实施。以上这些启示为云计算环境下学术信息资源共享安全保障提供了设计思路，在接下来的论述中，将以此为依据进行云计算环境下学术信息资源共享安全保障机制研究。

2 基于学术信息资源共享流程的安全技术保障机制

根据云计算环境下学术信息资源共享流程，在分析学术信息资源共享安全要素及其交互作用的基础上，在各个共享环节布置安全保障措施，形成基于学术信息资源共享流程的安全技术保障机制，如图 3 所示。

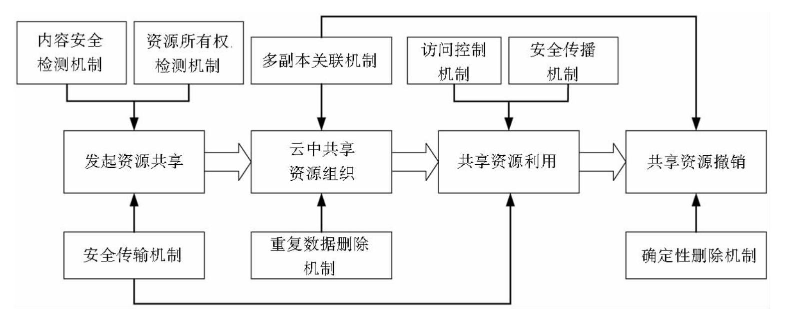


图 3 基于学术信息资源共享流程的安全技术保障机制

2.1 资源共享发布安全机制

在学术信息资源所有者发布资源共享时，为保障其安全，可采用的安全技术保障机制包括学术信息资源内容安全检测机制、资源安全传输机制及信息资源所有权验证机制。用户发起共享的学术信息资源来源广泛，可以来自于自身知识或经验的总结，也可能来源于对互联网资料的整理，用户在进行资料汇总时可能会包含一些涉密内容或恶意代码等，需要在资源共享前对其安全进行检测。学术信息资源内容安全检测机制主要保障共享的学术信息资源不涉及国家军事、国计民生等敏感信息，同时保障共享的资源中不被嵌入恶意代码，避免用户利用共享资源时遭到安全入侵等现象的发生[9]。同时，虽然用户发起学术信息资源共享旨在资源互相交流和高效利用，但也需要保障学术信息资源所有者的知识产权，避免侵权现象发生，如未经作者允许对资源进行二次转发、修改等。因此在共享资源发布时，需根据设定信息资源所有权验证机制，确定资源的所有者并颁发资源所有者证明，保障共享资源在云平台中的安全[10]。此外，在共享资源传输过程中，由于构建专用的网络传输通道成本高，且不易实现，而通用的网络为保障资源不被破坏、篡改、拦截，通常采用学术信息资源安全传输机制，在通信双方之间建立加密通信，保障数据传输的机密性。

2.2 云中共享资源组织安全机制

存储于云平台的共享资源应采用合理的关联组织机制，以保障共享资源存储过程中的安全。对应的学术信息资源安全技术保障机制包括多副本关联机制和重复数据删除机制。共享资源与由单用户独自拥有的普通资源在存储过程中存在明显区别，普通存储与云平台中的资源属于用户私有资源，其存储、更改由用户个人决定。而共享资源的访问、编辑等多由多方共同决定，其他授权用户也可能再次分享、下载或转存共享的资源，因此在云平台中共享的学术信息资源普遍存在多副本文件。学术信息资源多副本问题不仅会增加云平台的存储开销，增加用户选择资源时的困难，而且会导致共享的资源不受资源所有者约束和控制，如资源的访问时间和对象失去控制等，产生共享资源在知识产权上的纠纷。因此，有必要对学术信息资源多副本现象进行控制，在进行共享资源存储过程中，可采用重复数据删除机制对共享资源副本数量进行控制[11-12]。其中，共享资源副本数量应与共享资源的应用范围和数量有关，当用户对共享资源请求数量较多时，为提高处理效率，可以适当增加副本的数量。同时采用多副本关联机制对云平台中的多副本资源进行关联管理，使学术信息资源在云平台中有序存储组织，保障共享资源的安全[13]。

chinaXiv:202301.00609v1

chinaXiv:202307.00069v1

2.3 云中共享资源利用安全机制

共享资源利用环节是学术信息资源共享的重要环节之一,此阶段存在的安全问题包括共享资源不可用、非授权用户非法获取资源信息、非法篡改共享资源、用户权限撤销安全等,如果不加以控制,会对资源共享安全造成不利影响,因此可以采用资源安全传输机制、访问控制机制与学术信息资源安全传播机制进行控制。其中共享资源的安全传输机制与共享资源发布时相同,保障共享资源传输过程中的完整性和保密性。云环境下的学术信息资源共享可以是广泛范围内的共享,也存在有限范围内的共享,如果用户越权访问或擅自修改共享资源,可能产生安全事故,因此需设计细粒度的访问控制机制。访问控制是提供有效、安全的资源访问的重要用户身份管理手段,可以让不同需求的用户通过统一的方式访问授权信息,防止非授权信息访问,并提供集中式的数字身份管理、认证[14-15]。云环境下的访问控制机制可以保障用户身份安全,帮助云服务商确认用户身份的真实性、合法性,一般可在用户注册账户时完成对不同用户的授权,并通过用户提交登录信息验证其身份。学术信息资源安全传播机制主要保障共享资源在传播过程中学术信息资源所有者的知识产权不受侵害及相关敏感信息不被挖掘,在实现过程中主要通过对用户权限的控制来完成。

2.4 共享资源撤销安全机制

共享资源撤销是学术信息资源共享流程中的最后环节,此阶段主要采用学术信息资源多副本关联机制与共享资源确定性删除机制对其安全进行保障。当学术信息资源所有者完成共享并对共享资源进行撤销时,为保障其知识产权安全,应实现根据共享资源所有者的需求对所有副本资源关联删除操作。学术信息资源多副本关联机制作用于共享资源被其所有者撤销之后,云平台通过利用相关技术对共享资源的副本文件进行处理,删除全部副本资源及其备份文件。同时,由于云服务商对共享资源进行统一存储,当存储数据被删除时,云服务提供商将对应的存储空间分配给其他租户,原来云存储数据有可能被新租户恢复,此外也可能存在原有数据的备份没有在第一时间删除,导致学术信息资源共享资源泄露,因此,需要采用确定性删除机制,当共享资源被撤销时,保障包括云服务商在内的任何机构或个人无法将数据进行恢复[16]。在具体实施的过程中,可根据共享资源的保密性等级进行。

3 基于多主体协同的学术信息资源共享安全保障组织机制

学术信息资源共享安全保障需要适应其保障主体的多元化,传统的IT环境下,学术信息资源共享是在各学术信息资源服务机构中进行,其共享安全保障也依赖于各服务机构。云计算环境下,部分安全保障措施移交到云服务商进行统一部署,资源利用过程也转移到云中进行,造成云服务提供商与资源利用者也参与到学术信息资源共享安全保障之中。因此,云计算环境下,学术信息资源共享安全保障组织由多主体的协同参与,由此形成了基于多主体协同的学术信息资源共享安全保障组织机制。如图4所示:

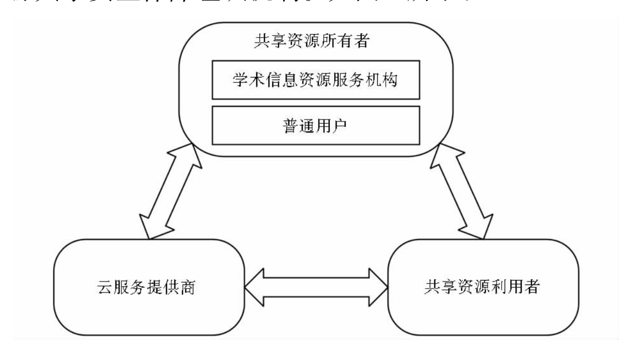


图4 基于多主体协同的学术信息资源保障组织机制

3.1 学术信息资源共享安全保障中的协同主体及定位

学术信息资源共享安全保障中的各类主体包括共享资源所有者、云服务提供商及共享资源利用者。其中,共享资源所有者在共享安全保障中处于主导地位,云服务提供商及学术信息资源利用者作为协同者参与到学术信息资源共享安全保障之中。

共享资源所有者是学术信息资源共享安全的最终负责人,因此,在进行共享安全保障组织过程时,共享资源所有者应充分发挥其主导作用,做好共享安全组织技术与管理规范,并通过与云服务提供商及共享资源利用者的协同保障学术信息资源共享安全的顺利进行。共享资源所有者由学术信息资源服务机构及普通用户构成,其中学术信息资源服务机构由商业性学术信息资源服务机构、公共图书馆、高校图书馆、科技情报中心等构成,其资源多为规范性的学术论文、科研数据、工具软件等,普通用户通过向云平台中上传共享资源完成学术信息资源共享,资源内容包括用户的个人知识总结、实验数据等。共享资源所有者在履行其主导作用时,需要对学术信息资源共享安全管理的范围和体系做出明确规定,包括共享安全策略的制定、共享

ChinaXiv合作期刊

安全风险评估及内容、风险控制目标与方式选择等，同时也需考虑云计算环境对共享安全保障的影响，制定面向云计算的学术信息资源共享安全技术保障机制和管理方式。

云计算环境下，云服务提供商与共享资源利用者作为共享安全协同保障的主体，从多个方面参与到学术信息资源共享安全保障之中，其中云服务提供商通过部署安全措施的方式直接参与，共享资源利用者则主要通过保障自身的账户安全、合理利用权限及多种形式的安全监督参与其中。云服务提供商拥有较为完备的技术资源和管理能力，是学术信息资源共享安全保障中的协同机构，直接参与共享安全保障的执行，具体工作包括保障学术信息资源共享服务的基础环境安全及学术信息资源共享过程中的共享资源安全两个方面。其中，学术信息资源共享服务的基础环境安全包括云平台的物理环境、硬件、虚拟化、网络、传输、学术信息资源服务主体账户、业务可持续性等方面的安全，这方面的要求需要视具体的服务情况及采用的云服务类型确定。学术信息资源共享过程中的共享资源安全主要从共享服务的角度，完成共享资源的组织及人员的管理，采用安全技术与管理措施相配合的方法，对云平台中资源共享的操作流程及共享资源的组织存储进行规范，保障共享过程中的安全。此外，云服务提供商还应主动提供支持进行共享资源安全管理控制，包括主动提供相关管理操作指南、向资源所有者提供相应安全防护工具、进行账户安全监测与异常提醒工作等。共享资源利用者可称为学术信息资源共享云平台中的用户，是共享资源的最终流向。在共享资源安全保障中，共享资源利用者不仅需要注重保障自身账号安全，不主动泄露个人信息，避免多个账号同一密码的情况，还应注意自身权限的利用，不滥用权限将个人账号转借他人等。此外，由于共享资源利用者的总体规模庞大，用户普遍能够及时发现各种安全问题，因此通常作为监督者参与学术信息资源共享安全保障之中，包括向云服务提供商和资源所有者报告安全问题等。

ChinaXiv:202307.00069v1

3.2 学术信息资源共享安全保障的协同机制

学术信息资源共享安全保障的协同机制是在共享资源所有者主导下的多主体协同机制，既包括共享资源所有者与云服务提供商、共享资源利用者的协同，也包括云服务提供商与共享资源利用者的协同。

在共享资源所有者与云服务提供商的协同方面，学术信息资源共享安全保障由共享资源所有者与云服务提供商分工进行，分别部署安全保障措施，同时，共享资源所有者应从管理和技术两方面，监督云服务提供商的安全保障工作，当出现安全事故时，首先对其原因进行全面分析，在此基础上进行责任认定。此外，共享资源所有者与云服务提供商还需建立高效的安全问题沟通机制，在安全保障实践中，存在一些安全措施的部署和安全事件的处理需要双方配合完成，为达到工作效益比的最优化，应从双方的响应机制和合作机制入手，优化工作流程，从而方便双方及时进行安全问题交流，避免安全事故发生。在共享资源所有者与共享资源利用者的协同方面，共享资源利用者的权限是有限的，因此并不直接对共享资源安全进行保障，但作为共享资源及共享服务的直接使用者，用户往往能够更为全面地感知各种安全问题，因此需要在保证用户账户及权限利用安全的情况下，需要建立共享资源所有者与广大用户之间的协同机制，鼓励他们通过正当的渠道和方式对共享中的安全保障措施进行监督，以便及时发现并解决安全问题。云服务提供商与共享资源利用者间的协同可通过建立用户意见反馈方式进行，当用户遇到问题时，可以通过特定渠道或方式向云服务提供商反映，比如设立专有意见反馈平台、问题投诉电子邮件、在线客服等。云服务提供商获取用户反馈的各种安全问题后，应及时做出响应，从而避免安全事故发生或范围扩大。

4 结论

为适应云计算环境下的学术信息资源共享，构建与云计算环境相适应的学术信息资源共享安全保障机制，本文在分析云计算环境下学术信息资源共享流程及其安全要素的基础上，提出了基于学术信息资源共享流程的安全技术保障机制及基于多主体协同的学术信息资源共享安全保障组织机制，从而保障学术信息资源共享中的各主体安全，降低资源共享过程中的安全风险。

参考文献：

[1] 文庭孝，陈能华. 信息资源共享及其社会协调机制研究[J]. 中国图书馆学报，2007，33(3)：78–81.

[2] 全国信息安全标准化技术委员会. 信息安全技术 信息安全风险评估规范：GB/T 20984–2007[S]. 北京：中国标准出版社，2007.

[3] JITHIN R，CHANDRAN P. Virtual machine isolation[M]// MARTÍNEZ PÉREZ G，THAMPI S M，KO R，et al. Recent trends in computer networks and distributed systems security. Berlin：Springer，2014：91–102.

[4] BIRJE M N，CHALLAGIDAD P S，GOUDAR R H，et al. Cloud

computing review: concepts, technology, challenges and security [J]. International journal of cloud computing, 2017, 6(1): 32 – 57.
[5] 蒋洁. 云数据安全风险与规制框架[J]. 情报资料工作, 2013(1):57 – 60.
[6] 张玉清, 王晓菲, 刘雪峰,等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6):1328 – 1348.
[7] ALI M, DHAMOTHARAN R, KHAN E, et al. SeDaSC: secure data sharing in clouds[J]. IEEE systems journal, 2017, 11(2): 395 – 404.
[8] 王于丁,杨家海,徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报,2015,26(5):1129 – 1150.
[9] 刘梅彦, 黄改娟. 面向信息内容安全的文本过滤模型研究[J]. 中文信息学报, 2017, 31(2):126 – 131.
[10] BARSOUM A F, HASAN M A. Provable multicopy dynamic data possession in cloud computing systems[J]. IEEE transactions on information forensics & security, 2017, 10(3):485 – 497.
[11] YANG C, REN J, MA J. Provable ownership of files in deduplication cloud storage [J]. Security and communication networks, 2015, 8(14): 2457 – 2468.
[12] 熊金波, 张媛媛, 李凤华,等. 云环境中数据安全去重研究进展[J]. 通信学报, 2016, 37(11):169 – 180.
[13] 熊金波, 沈薇薇, 黄阳群,等. 云环境下的数据多副本安全共享与关联删除方案[J]. 通信学报, 2015, 36(S1):136 – 140.
[14] XU S, YANG G, MU Y, et al. Secure fine-grained access control and data sharing for dynamic groups in cloud[J]. IEEE transactions on information forensics & security, 2018, 13(8): 2101 – 2113.
[15] 宋国峰, 梁昌勇. 一种基于用户行为信任的云安全访问控制模型[J]. 中国管理科学, 2013(S2):669 – 676.
[16] 冯贵兰, 谭良. 基于信任值的云存储数据确定性删除方案[J]. 计算机科学, 2014, 41(6):108 – 112.

作者贡献说明:
石宇:设计研究方案,撰写论文;
胡昌平:提出问题,指导和修改论文。

Comprehensive Security Guarantee Mechanism for Academic Information Resources Sharing in the Cloud Computing Environment

Shi Yu Hu Changping
School of Information Management of Wuhan University, Wuhan 430072

Abstract: [**Purpose/significance**] In order to guide the implementation of sharing security guarantee, this paper constructs the whole-process security guarantee mechanism for academic information resources sharing in cloud computing environment from the perspective of technology and management. [**Method/process**] On the basis of analyzing the process and security elements of academic information resources sharing in the cloud computing environment, this paper designs a comprehensive security mechanism of academic information resources sharing. [**Result/conclusion**] The security technology mechanism is proposed based on the processing of academic information resources sharing, and the security organization mechanism of academic information resources sharing based on multi-agent collaboration.

Keywords: cloud computing environment academic information resources sharing security guarantee mechanism

chinaXiv:202307.00609v1

“名家视点”第8辑丛书书讯

由《图书情报工作》杂志社精心策划和主编的“名家视点”系列丛书第8辑已正式出版。该系列图书资料翔实,汇集了多位专家的研究成果和智慧,观点新颖而富有见地,反映众多图书馆学情报学热点和前沿研究的现状及发展趋势,对理论研究和实践工作探索均具有十分重要的参考价值和指导意义,可作为图书馆学情报学及相关学科的教学参考书和图书情报领域研究学者和从业人员的专业参考书。该专辑的4个分册信息如下,广大读者可直接向本杂志社订购,享受9折优惠并免邮资。

- 《智慧城市与智慧图书馆》(定价:52.00)
- 《面向 MOOC 的图书馆嵌入式服务创新》(定价:52.00)
- 《数据管理的研究与实践》(定价:52.00)
- 《阅读推广的进展与创新》(定价:52.00)

欢迎踊跃订购!
地　址:北京中关村北四环西路33号5D室
邮　编:100190
收款人:《图书情报工作》杂志社
电　话:(010)82623933
联系人:谢梦竹　王传清